

A WHITE PAPER

Federal Continuity of Operations

Part 3 of 10: The Business Impact Analysis



Topic Summary:

- The Business Impact Analysis as related to Continuity of Operations
- Business Impact Analysis methodologies compared
- Determining Mission Essential Functions
- Summary and Recommendations for next steps

Table of Contents

1.0	Introduction.....	1
2.0	Mission Essential Functions (MEFs) and the Business Impact Analysis (BIA).....	1
2.1	Relating COOP to the BIA	1
2.2	Methodology 1: BS 25999-1:2006 - Business Continuity	2
2.3	Methodology 2: NIST 800-34 - Contingency Planning Guide for Federal Information Systems.....	4
2.3.1	Determine mission/business processes and recovery criticality	5
2.3.2	Identify Resource Requirements.....	6
2.3.3	Identify System Resource Recovery Priorities.....	6
2.4	Methodology 3: DoDI 3020.42 - Defense Continuity Plan Development.....	7
3.0	Concluding Remarks	9
3.1	Summary	9
3.2	Recommendations	9
3.3	Next Steps	10
	Appendix A: Acronyms and Abbreviations	11
	About the Author.....	12
	Reference List	12

Illustration Index

Figure 1: NIST's BIA Approach	5
-------------------------------------	---

Table Index

Table 1: BS 25999-1:2006 BIA Guidelines	2
Table 2: Example NIST Information System Resource/Component Table	6
Table 3: DoDI 3020.42 MEF Identification Guidelines	7
Table 4: Recommendations	9

1.0 Introduction

An organization must identify its critical business functions using a Business Impact Analysis (BIA) prior to implementing a Business Continuity Management (BCM) plan. The same requirement exists within federal government and Department of Defense (DoD) agencies with a significant difference: these agencies must preserve their ability to accomplish their mission rather than their ability to retain revenue. Hence, federal government and DoD agencies implement a Continuity of Operations (COOP) plan by determining their Mission Essential Functions (MEFs). This paper, the third in a ten-part series, analyzes how a small Army Program performs the government equivalent of a BIA to determine its MEFs and to determine protections.

Neither the federal government, DoD, nor the Army define how a particular agency should determine its MEFs and prioritize them to meet policy requirements. This paper analyzes three different good-practice methodologies that enable the agency to identify and prioritize its MEFs in preparation for a formal Risk Assessment of the threats and hazards that face those MEFs. The paper closes by summarizing its findings presenting recommendations for the program manager (PM) to review.

2.0 Mission Essential Functions (MEFs) and the Business Impact Analysis (BIA)

This section correlates how the commercial-based concept of the BIA relates to the government-based concept of the MEF. It also explores three different methodologies in common use for determining the operational impact of various functions on an organization, which is a need common to the commercial and the government worlds.

2.1 Relating COOP to the BIA

British Standard 25999-1:2006 (“Business Continuity”) is a good-practice standard for ensuring business continuity and defines the Business Impact Analysis (BIA) as a foundational element of BCM which:

identifies, quantifies and qualifies the business impacts of a loss, interruption or disruption of business processes on an organisation and provides the data from which appropriate continuity strategies can be determined (GPG08-2, p 5).

Within the federal government and DoD, the BIA is not labeled as such within policy statements for a very practical reason. Namely, commercial organizations are concerned with protecting revenue-generating ability; after some period of time without revenue, the commercial firm ceases to exist. The government and DoD are concerned with fulfilling their mission of fulfilling their mission: ensuring the continuous operation of our system of government in all circumstances.

Frankly, BCM within the commercial world does a better job at pointing out the difficulty in identifying “critical functions” than the federal government and in providing solid recommendations for performing an impact analysis. In keeping with the use case for this series of white papers, consider the U.S. Army COOP doctrine (Regulation 500-3, U.S. Army Continuity of Operations Program Policy and Planning), which derives directly from the DoD (Instruction 3020.26, “Department of Defense Continuity Programs”), which in turn derives from the Executive branch (National Security and Homeland Security Presidential Directive NSPD-51 / HSPD-20,

“National Continuity Policy”). The Army regulation simply states:

- “Identify and prioritize MEFs in accordance with MEF definitions and guidance contained within this regulation to be performed as the basis for continuity planning, preparation, and execution” (p 7).
- “Identify and prioritize organizational MEF” (p 11).
- “Identify and prioritize MEFs necessary to execute during emergencies” (p 13).
- “Identify organizational MEFs that can be deferred without impact to the unit’s core mission until the situation permits their execution” (p 13).

The above instructions do not help the Army agency or program in determining exactly what functions are mission-essential, nor does the Army Regulation (AR) provide guidance on how the agency or program would determine its indirect impacts (for example, functions provided by other groups that an MEF depends upon). The commercial world, however, has numerous methodologies that exist to assist the organization in identifying and prioritizing its critical functions; these same techniques can assist government organizations as well. This section briefly compares three such BIA methodologies.

2.2 Methodology 1: BS 25999-1:2006 - Business Continuity

BS 25999-1:2006 provides a generalized code of practice for implementing BCM. Section 2 of the Good Practice Guidelines from the Business Continuity Institute provides an overview of the BIA, which must “identify the timescale and extent of the impact of a disruption at several levels in an organization” (GPG08-2, p 5). The BIA’s purpose is to understand and document formally how specific functional losses affect the organization over time and to inform decision makers about maximum tolerable outages. Just as importantly, the BIA must identify the dependencies that identified critical functions have on other functions (perhaps ostensibly less critical). Furthermore, the BIA must be a living document with regularly scheduled updates.

The methodology can be summarized as follows:

Table 1: BS 25999-1:2006 BIA Guidelines¹

BS 25999-1:2006 Guideline		Applied to Use Case (Army Program)
Step	Element	
1	Obtain the full support of an executive sponsor prior to performing the BIA.	Locate Commanding Officer (CO) or <i>authorized deputy</i> to provide authority for the analysis.
2	Create the BCM Policy	Refer to AR 500-3 for guidance
3	Identify discrete business activities across the organization	In conjunction with the CO or deputy, use AR 500-3 to determine an initial list of higher-level functions and their owners.
4	Identify suitable staff from whom information can be sought about the business processes – subject matter	Interview functional owners for a list of SMEs.

¹ The British spelling within the listed BS 25999-1:2006 elements is taken from the standard.

BS 25999-1:2006 Guideline		Applied to Use Case (Army Program)
	experts (SMEs)	
5	Identify the impacts which may result in damage to the organisation's reputation, assets or financial position	Craft scenarios and interview questions for the identified SMEs to determine MEFs.
6	Quantify the timescale within which the interruption of each business activity becomes unacceptable to the organization	Rank each MEF from A to D ²
7	Where an organisation has multiple sites it may be necessary to decide on the maximum geographic extent of a disruption or extent of resource loss that the organisation wants to, or needs to, plan to survive to quantify impact.	COOP capabilities depend upon the relative ranking of each MEF. An MEF ranked "A" must continue to operate no matter how widespread a disruption might be.
8	Obtain sign-off by the process owner to confirm accuracy of information	Collate data and present to functional owners. Allow a controlled period of time for discussion and comments.
9	Obtain support of the BCM sponsor for the conclusions	Present the findings to the CO; due to the hierarchical Army environment implementing the COOP Program from these findings may very well require multiple levels of funding approval (all the way up to the Congressional level).

The abstract BIA methodology specified by BS 25999-1:2006 thus relates closely to an approach useful to the Army in particular and DoD / federal government in general.

² AR500-3: Priority A MEFs are tasks that must continue without interruption. These are MEFs of such importance that they must continue to be performed regardless of what is happening around the organization or in the world. Priority B MEFs are tasks that an agency can defer no longer than 48 hours from "N" time (see NOTE below); priority C MEFs are tasks that an agency can defer for no longer than 7 days from "N" time; and priority D MEFs may be deferred until the COOP event is over and normal unit operations are restored (p 13).

2.3 Methodology 2: NIST 800-34 - Contingency Planning Guide for Federal Information Systems

The National Institute of Standards and Technology (NIST), under the aegis of the Commerce Department, provides guidance to the Executive branch on standards for everything “from automated teller machines and atomic clocks to mammograms and semiconductors.”³ While NIST’s guidance is non-regulatory, numerous DoD regulations derive from or have influenced NIST Special Publications (SPs) and Interagency Reports (IRs).

SP 800-34 (“Contingency Planning Guide for Federal Information Systems”) provides an information technology (IT) focused guide on ensuring the confidentiality, availability, and integrity of federal information systems “from minor incidents causing short-term disruptions to disasters that affect normal operations for an extended period” (p 16). Interestingly, the SP explicitly disassociates itself from both disaster recovery and COOP planning “except where it is required to restore information systems and their processing capabilities.” In fact, the guide does not address mission-level or business-function continuity at all. That being said, the techniques presented within the SP to identify the critical components of an information system are of great value for Army, DoD and federal agencies or programs.

The SP clearly delineates between *continuity planning* (“the ability to continue critical functions and processes during and after an emergency event”) and *contingency planning* (“provides the steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency”).⁴ In NIST’s opinion, an Information System Contingency Plan (ISCP) may be necessary as a subset of the overall COOP Program, but the two are fundamentally different creatures. The ISCP exists to satisfy Federal Information Security Management Act (FISMA) requirements, while COOP exists to satisfy NSPD-51 / HSPD-20.

In another break with federal, DoD, and Army COOP policies, the SP uses the term “Business Impact Analysis” to describe how implementers should analyze information system components. In actual fact, the SP references Federal Continuity Directive (FCD) 2 (“Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process”) for implementers to perform a *process-focused BIA* as opposed to the SP’s *system-focused BIA*.

The Army Program use case addressed by this set of white papers primarily concerns itself with continuity of operations for the proper functioning of an information system rather than the entire set of business systems. Therefore, the NIST SP provides especial value in its three-tiered BIA approach:

- Determine mission/business processes and recovery criticality;
- Identify resource requirements; and,
- Identify recovery priorities for system resources.

³ NIST, “NIST General Information,” *NIST Web site*, October 5, 2010. Available at: http://www.nist.gov/public_affairs/general_information.cfm (last accessed: June 22, 2011).

⁴ SP800-34, p 21.

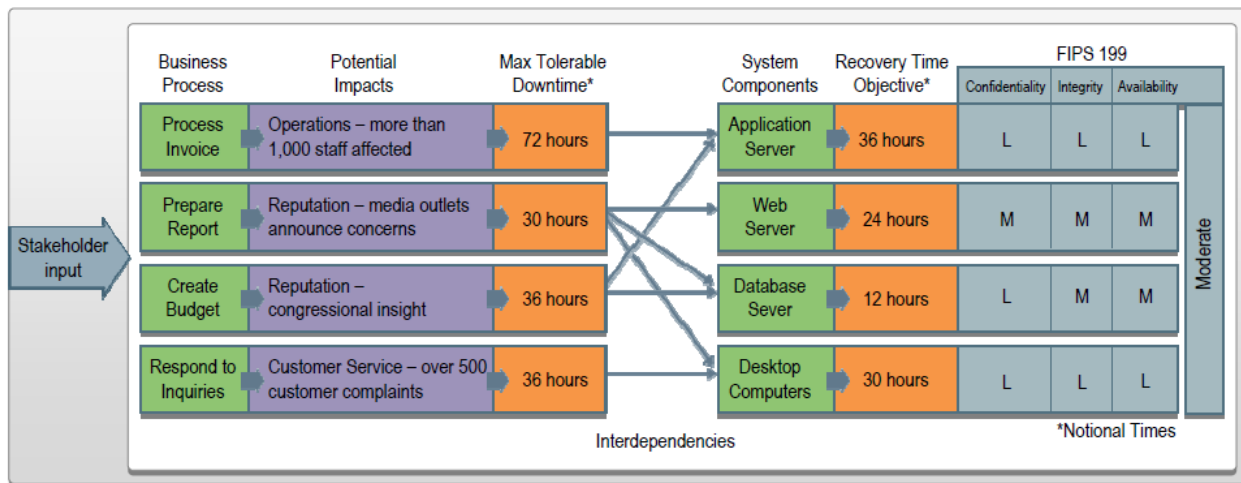


Figure 1: NIST's BIA Approach

The following sections analyze NIST’s BIA approach in more detail.

2.3.1 Determine mission/business processes and recovery criticality

NIST’s first step is to determine which mission processes exist and to rank them appropriately. NIST’s SP does not provide guidance on how to perform this identification and ranking because the SP focuses on the information systems that support critical mission processes. One important addendum not mentioned within BS 25999-1:2006 is the need to look at supporting information systems and their security impact. NIST’s Federal Information Processing Standard (FIPS) 199 (“Standards for Security Categorization of Federal Information and Information Systems”) provides guidance for this evaluation (low, medium, or high) based on the information system’s potential impact on the nation in the event of disclosure. These system data categorization criteria can help to inform the practitioner of the related criticality of a business process.

Moreover, the Army Program benefits from NIST’s emphasis on establishing impacts based on “values or units of measurement that are meaningful to the organization” (SP800-34, p 31). The goal is to determine the following (p 31):

- Maximum Tolerable Downtime (MTD). The total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations.
- Recovery Time Objective (RTO). RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD.
- Recovery Point Objective (RPO). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage.

2.3.2 Identify Resource Requirements

As with the BS 25999-1:2006 approach, NIST recommends that the practitioner work with the SMEs to identify what specific resources are required to operate a given function. Unlike BS 25999-1:2006, NIST’s approach is IT system-centric and provides a valuable add-on for ensuring that the technical expertise exists to run a program from a remote site if a COOP is declared.

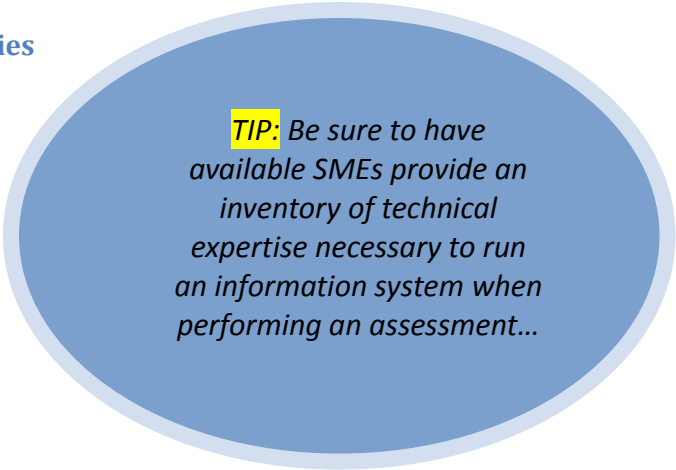
An example table follows:

Table 2: Example NIST Information System Resource/Component Table

System Resource / Component	Platform/OS/Version (as applicable)	Description	Resources
Data Services Server	Linux RHEL 5.4 running Apache 2.54	In-house application with custom data services invoked by Providers	Linux System Admin In-house Application
Collaboration Portal	Windows Server 2008 R2 running SharePoint 2010	Uses standard and customized Webparts; ties into organizational database	SharePoint Admin Server 2008 Admin In-house Developer

2.3.3 Identify System Resource Recovery Priorities

Recovery priorities in NIST’s SP constitute the final BIA step and offer the least value to the practitioner. NIST simply declares that “priorities can be effectively established taking into consideration mission/business process criticality, outage impacts, tolerable downtime, and system resources” (p 33). The onus of how these priorities are determined falls upon the implementer. SMEs can be of especial value simply by listing the technical roles required for each information system technology.



TIP: Be sure to have available SMEs provide an inventory of technical expertise necessary to run an information system when performing an assessment...

2.4 Methodology 3: DoDI 3020.42 - Defense Continuity Plan Development

Unlike the bare policy statements from DoD Instruction 3020.26, DoD Instruction 3020.42 provides a clear roadmap for determining what constitute mission essential functions as well as the necessary steps for ensuring that these functions can be met in the face of an emergency. In short, much the same results as a commercial BIA should provide.

The Instruction begins by defining *capabilities* (“[c]ommunications, facilities, information technology, trained personnel, and other assets necessary to conduct mission essential functions (MEF) and supporting activities.”) and *supporting activities* (“[t]hose **specific activities** that a department or agency **must conduct** in order to **perform its MEF**”).⁵ These activities correspond closely to the concept of “activity” within a commercial BIA.

The Instruction then proceeds to define the set of procedures to enable the department or agency to accomplish its mission; Sections 6.1.1 (“Identify MEF”), 6.1.2 (“Identify Supporting Activities”), 6.1.3 (“Identify Vital Records”), and 6.1.4.1 (“Identify the position requirements necessary to perform MEF”) provide the basis for DoD methodology. (The remaining 6.x Sections within the Instruction relate to *implementing* the COOP Program as opposed to performing an impact analysis.) Similarly to the BS 25999-1:2006 methodology, these steps can be related to the Army Program use case:

Table 3: DoDI 3020.42 MEF Identification Guidelines

DoDI 3020.42 MEF Identification Guideline Element		Applied to Use Case (Army Program)
Step	Element	
6.1.1.1	List all the Component functions that have the <i>potential</i> to be considered essential to the mission, to include: Command and Control; Command decision making capability; Crisis communications; Crisis data storage; Legal, fiscal, and contractual obligations; Personnel; Support to other DoD agencies.	In conjunction with the Commanding Officer (CO) or authorized deputy, identify high-level functions and their owners. Receive authority to interview / survey these owners to build an interdependent list of Program functions.
6.1.1.2	Establish functional criticality by examining the consequences of nonperformance.	This differs greatly from the commercial model; this analysis is qualitative and does not refer to financial impact. Within the Army Program, this translates to identifying the dependent stakeholders (data Consumers) and their needs for each managed system / process. Downstream liability determines the evaluated prioritization. As a project manager for the Army Program put it, “Nonperformance that affects the Warfighter, no matter

⁵ DOD-3020, p 1 (emphasis added).

DoDI 3020.42 MEF Identification Guideline Element		Applied to Use Case (Army Program)
		what the cause, leads directly to penalties and lost future opportunities.” ⁶
6.1.1.3	Prioritize plans focused upon “mission essential” functions only; ensure that functions meeting MEF status can be restored no later than 12 hours from a COOP declaration.	From a budgeting standpoint, “MEF” at the DoD policy level can be inferred to mean “supporting a National Essential Function (NEF).” ⁷ Because smaller programs will not meet the standard for this definition, the local Commander will need to present COOP funding up the approval chain after determining and prioritizing the local MEFs. A smaller program will not receive approved funding for 12 hour recovery in a true national disaster, but COOP funding will still be available to handle smaller events.
6.1.2	Identify Supporting Activities.	These activities establish the “upstream” dependencies of the Army Program. For example, access to a managed information system probably requires Army Knowledge Online (AKO) to be functioning in order for Army users to login to the system. The goal is to determine the dependency tree for each local MEF.
6.1.3	Identify Vital Records.	BS 25999-1:2006 repeatedly emphasizes the need for the organization to protect its vital records. For the Army Program, these vital records include its network authorizations, data supplier agreements, signed vendor contracts, and more. In the absence of these records, the organization cannot fulfill its mission.
6.1.4.1	Identify the position requirements necessary to perform MEF.	The Army Program must ensure that it has the appropriate personnel in-place to accomplish its mission from (potentially) an alternate location. The implementation

⁶ Source: Personal interview with the contractor’s project manager, June 29, 2011.

⁷ HSPD-20, p 2: “National Essential Functions,” or “NEFs,” means that subset of Government Functions that are necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through COOP and COG capabilities.”

	DoDI 3020.42 MEF Identification Guideline Element	Applied to Use Case (Army Program)
		plan would specify who these people are (via personnel rosters) while the BIA specifies what roles must be filled (for funding and planning purposes).

The DoD COOP impact analysis methodology’s roots in BS 25999-1:2006 can be discerned clearly. The fundamental difference using DoD’s approach lies in the sole reliance on qualitative judgments to determine mission criticality, and the COOP Practitioner does well to bear this in mind.

3.0 Concluding Remarks

3.1 Summary

Army, DoD, and federal COOP policy statements do not provide sufficient guidance to COOP practitioners in determining exactly what constitutes an organization’s mission essential functions. This paper has analyzed how the commercially-focused BIA can be applied to COOP in general, and to this paper’s Army Program in particular. Three methodologies were identified: BS 25999-1:2006 (“Business Continuity”), NIST SP 800-34 (“Contingency Planning Guide for Federal Information Systems”), and DoD Instruction 3020.42 (“Defense Continuity Plan Development”).

The BS 25999-1:2006 approach provides a solid set of steps to perform a BIA, where each step can be correlated to the Army Program’s specific needs. NIST’s approach provides valuable additional insight into determining the business impact of underlying supporting information systems, especially where those information systems store classified data that whose disclosure could have a significant negative impact on the nation. DoD’s Instruction 3020.42 helps by providing a set of procedures for determining just exactly what constitute mission essential functions.

The combination of all three of these methodologies provides the COOP practitioner with a standards-based set of tools and techniques for ensuring that mission essential functions are thoroughly understood from two views: the business process (the mission function being performed), and the system process (the supporting infrastructure ensuring that the business process can be performed).

3.2 Recommendations

This paper has examined several methodologies for performing a BIA within the context of a COOP Program, and has provided a number of recommendations as shown in the table below:

Table 4: Recommendations

Recommendation	Rationale
<i>Start by reviewing commercial standards</i>	The federal government and DoD depend on blanket statements instructing the implementing organization to identify MEFs. The commercial standards have roadmaps in place specifically designed to help an organization in doing this identification.

Recommendation	Rationale
<i>Locate the most relevant individual for sponsorship</i>	In the commercial world, a funding sponsor is essential to creating a BCM program. In the public sector, the “funding sponsor” may well be at the Cabinet level so it makes sense to locate an individual who can give preliminary approval to move forward. The COOP Practitioner must keep this person informed at all times on the state of the project, and will do well to make the COOP Plan implementation a series of much smaller and time-focused projects.
<i>For information systems supporting the Army Program, perform a system-focused BIA</i>	A system-focused BIA should be <i>contingency-biased</i> in that it is designed to provide a procedure for recovering the operation of the supporting information system in an emergency. The NIST Special Publications provide a wealth of information for the COOP Practitioner to use when performing the BIA; analyzing the underlying information systems often results in additional MEFs and dependencies being uncovered.
<i>Perform qualitative assessments within government / DoD to determine MEFs</i>	DoD policy clearly states that a MEFs criticality is based solely upon the impact caused by that functions nonperformance. This is vastly different from the commercial world and should remind the COOP Practitioner that the emphasis is on ensuring smooth continuity of government functions. The Army is an executing arm of the U.S. government, and thus falls under the umbrella of “supporting functions” for ensuring Continuity of Government.
<i>Make the BIA part of a set of smaller COOP Plan projects.</i>	A small program will only rarely meet the high-level standard for an NEF (or NEF supporting function); thus causing funding difficulties for that program’s COOP Plan. The COOP Practitioner should respect that constraint and present a staggered COOP Plan implementation schedule where the BIA is an affordable part.

3.3 Next Steps

The next paper in this series will identify how the small Army program can use the output from the BIA (the prioritized critical functions, along with their maximum tolerable outage details) to perform a Risk Assessment. These critical functions are at danger from some set of threats (manmade, such as thieves and terrorists) and hazards (natural, such as floods or tornadoes), and the Risk Assessment helps the organization to quantify the *risk* (probability and impact) of a given set of threats / hazards.

Appendix A: Acronyms and Abbreviations

<i>AKO</i>	Army Knowledge Online
<i>AR</i>	U.S. Army Regulation
<i>BCM</i>	Business Continuity Management
<i>BIA</i>	Business Impact Analysis
<i>BS</i>	British Standard
<i>CO</i>	Commanding Officer
<i>COOP</i>	Continuity of Operations
<i>DoD</i>	Department of Defense
<i>FCD</i>	Federal Continuity Directive
<i>FISMA</i>	Federal Information Security Management Act
<i>HSPD</i>	<i>(National Security and)</i> Homeland Security Presidential Directive
<i>ISCP</i>	Information System Contingency Plan
<i>IT</i>	Information Technology
<i>MEF</i>	Mission Essential Function
<i>MTD</i>	Maximum Tolerable Downtime
<i>NIST</i>	National Institute of Standards and Technology
<i>NSPD</i>	National Security Presidential Directive
<i>RPO</i>	Recovery Point Objective
<i>RTO</i>	Recovery Time Objective
<i>SME</i>	Subject Matter Expert
<i>SP</i>	Special Publication
<i>U.S.</i>	United States

About the Author

Andrew Bruce is a Lead Scientist for Computer Sciences Corporation (CSC) in the Army Programs group of the North American Public Sector. CSC provides professional services to the Federal Government and the Department of Defense, specializing in customizing and developing architecture and governance models that enable tight integration to the Army's enterprise portfolio management initiatives. Mr. Bruce's job responsibilities include: working directly with customers and partners for new business development, supporting proposal efforts, overseeing Army customers' network infrastructure, working with project managers to ensure project completion, managing software development efforts throughout the entire system life-cycle, and leading new technology research and proofs-of-concept. After a career spanning three decades in shrink-wrap, commercial, and corporate software development, Mr. Bruce is focusing on Information Assurance to achieve his goal of building and managing large data centers providing cloud computing utility services for commercial and Government customers. Mr. Bruce holds the CISSP, PMP, and FITSP-D certifications and is currently pursuing a Master's Degree in Information Assurance from Norwich University.

Reference List

- [AR500-3] Department of the Army. April 18, 2008. Army Regulation 500-3: U.S. Army Continuity of Operations Program Policy and Planning. <<http://www.fas.org/irp/doddir/army/ar500-3.pdf>>. Accessed: June 12, 2011. 39 p.
- [DOD-3020] Department of Defense. February 17, 2006 (Certified current as of April 27, 2011). DODI 3020.42: Defense Continuity Plan Development. <<http://www.dtic.mil/whs/directives/corres/pdf/302042p.pdf>>. Accessed: June 21, 2011. 11 p.
- [GPG08-2] Business Continuity Institute. 2007. Good Practice Guidelines 2008: A Management Guide to Implementing Global Good Practice in Business Continuity (Section 2). Caversham (UK). 14 p.
- [HSPD-20] Bush, GW. May 9, 2007. National Security and Homeland Security Presidential Directive (NSPD 51 / HSPD-20): National Continuity Policy. White House: Office of the Press Secretary. 6 p.
- [ICOR] Business Continuity Services, Inc. 2009. Essentials of Business Continuity Management Series: The Business Impact Analysis (Week 3 Reading). ICOR: Lombard (IL). 80 p.
- [SP800-34] NIST. May 2010. Special Publication 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems. <http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf>. Accessed: June 21, 2011. 149 p.